Formatting Instructions Adversarial-ML Course

Abstract

The abstract paragraph is *optional* for the extended abstract and *mandatory* in the final project report.

1 Guidelines Extended Abstract and Final Project Report

1.1 Timeline – Dates Importantes

- March 5th (11:59PM AoE): Extended Abstract submission – Soumission du pré-rapport (**max 2 pages**).
- April 22th (11:59PM AoE): Project Report submission – Soumission du rapport de projet (**max 8 pages**).

Penalty policy: 10% of the grade per 24h late. Example: you submit your extended abstract on March 14th at 1:00 AM (AoE) you get a penalty of 10%. If you submit March 15th at 2:00 AM (AoE) you get a penalty of 20%.

Note that each time you edit your submission it *removes* the previous timestamp.

1.2 Details

The goal of the extended abstract is to separate the generation and confirmation of hypotheses. This process is inspired by the Pre-registation experiment NeurIPS 2020 workshop. The idea is to separate the formulation of a scientific hypothesis to its validation:

> *Pre-registration changes the incentives by reviewing [...] before experiments are conducted. The emphasis will be on whether the experiment plan can adequately prove or disprove one (or more) hypotheses. Some results will be negative, and this is welcomed. This way, good ideas that do not work will get welcomed. Finally, the clear separation between hypothesizing and confirmation will raise the statistical significance of the results.*

To summarize, the process is the following:

- Come up with a project (empirical or theoretical), you can take inspiration from the list of papers relevant for projects. The goal here is to pinpoint new questions.
- Write the extended abstract without confirmatory experiments/proofs by motivating this idea. (Providing context and motivations)
- Run the experiments/work on the proofs and report your results.

1.3 Pages limits

The extended abstract should be **maximum 2 pages long** (not including refs) and the final report should be **maximum 8 pages long** (not including refs). You can also have an appendix for proofs and additional results but the focus of the evaluation will be on the 8 pages of the main text. **Stephen Boyd LaTeX and project pieces of advice can be found here**. Spelling can be checked using grammarly.

1.4 Code

The code can be an important aspect of the project. If it is the case it *must* be part of the project report. The source can be shared with the project report but it is strongly advised to share a Github repository (or any other version control system) containing the frequent commits of code. Here is a summary of the guidelines:

1. A good practice is to start a Github repository as soon as possible and to frequently commit you updates on the code.
2. I advise you to use a strong IDE (integrated development environment). My advice is Pycharm (you can get a free license as a student) or Visual Studio Code.
3. It is fine to use some open-source code if you are transparent about it! (If you pretend it is your own code it is considered plagiarism)
4. If you need advice about the coding workflow/good practices come to the office hours.

Regarding the project contributions, doing a new experiment that is well-motivated and requires the design of some new code is a sufficient contribution to the project. The motivations and descriptions of the new experiment(s) should be presented in the extended abstract.

1.5 Resources

In order to access the feasibility of your project. You should roughly indicate the computational resources you will have access to (cluster, personal GPU, collab,...)

References with bibtex

Note that the Reference section does not count towards the number of pages of content that are allowed. Citations within the text must include the author's last name and year e.g., [Michalski et al., 1983]. Be sure that the sentence reads correctly if the citation is deleted: e.g., instead of "As described by [Duda et al., 2000], we first frobulate the widgets," write "As described by Duda et al. [2000], we first frobulate the widgets." The references listed at the end of the paper can follow any style as long as it is used consistently.

References

R. O. Duda, P. E. Hart, and D. G. Stork. *Pattern Classification*. John Wiley and Sons, 2nd edition, 2000.

R. S. Michalski, J. G. Carbonell, and T. M. Mitchell, editors. *Machine Learning: An Artificial Intelligence Approach, Vol. I.* Tioga, Palo Alto, CA, 1983.

A First Section of the Appendix

You can put technical proofs and additional experiments here.